Statewide Information Security Standards
Deviation Reporting Policy and Procedures

Purpose

This document describes the policy and procedures for reporting, reviewing and monitoring deviations to the Statewide Information Security Manual.

Scope

The scope of this policy and procedures is specific to the Enterprise Security and Risk Management Office (ESRMO) and all Executive Branch agencies, including the Office of Information Technology Services (ITS), which may have need to report an information security standards deviation to the Statewide Information Security Manual.

Deviation Reporting Policy

The Statewide Information Security Manual is the foundation for information technology security in North Carolina. It sets forth the information security standards required by G.S. §147-33.110, which directs the State Chief Information Officer (State CIO) to establish a set of statewide standards for information technology security to maximize the functionality, security, and interoperability of the State's information technology assets. The current version of the manual may be found on the State CIO's web site at the following page:

https://www.scio.nc.gov/mission/itPoliciesStandards.aspx.

The statewide information security standards have been extensively reviewed by representatives of each agency within the executive branch of state government and are annually reviewed as technology and security needs change. All agencies are expected to be familiar with and to comply with the information security standards set forth in the Statewide Information Security Manual. A deviation from a statewide information security standard is a situation in which an agency information technology resource is out of compliance with the Statewide Information Security Manual. A deviation to a statewide information security standard may put state information systems and/or data at risk of damage, loss or exposure.

Agencies must be aware of their deviations from statewide information security standards and need to regularly assess the risks associated with their deviations. Agencies shall report all known deviations to the Statewide Information Security Manual to the ESRMO for review. The deviation reporting process is designed for agencies to *report* deviations to the Statewide Information Security Manual that an agency should be actively working to resolve or mitigate. The process is not intended for an agency to *request* to deviate from a statewide standard or to report a permanent deviation to the Statewide Information Security Manual. There must be a compelling business need for an agency to allow a continuing information security standard

deviation. Each agency is responsible for evaluating the risk of an information security standards deviation, the justification for that risk, and any compensating measures taken to reduce the risk. The ESRMO also needs to be aware of deviations to the Statewide Information Security Manual so that staff can help agencies develop risk mitigation measures. The State CIO reviews all deviation reports and determines whether a deviation report is approved or denied and whether the agency is taking appropriate steps to mitigate risks associated with a deviation.

Deviation Review Process

Each agency shall use the Statewide Security Standards Deviation Report Form to report their deviations to the State CIO. The deviation report form may be found on the State CIO's web site at http://esrmo.scio.nc.gov/security/. The agency's Security Liaison is responsible for reviewing and approving the content within a deviation report form before submitting it to the ESRMO for review. The agency Security Liaison who submits a deviation report should understand that an information security standards deviation increases the risk of damage, loss or exposure to a state information system and/or data and that the agency accepts this risk. A deviation report must have a compelling justification with detailed plans for mitigating and resolving the deviation, as well as an estimated completion date for when the deviation will be resolved. **Note:** *All deviation reports are temporary and will have an expiration date*. A deviation report must also include an Enterprise Project Management Office (EPMO) project number whenever a deviation pertains to an enterprise project tracked by the EPMO.

The following is a list of information required for each deviation report:

- Agency and Division Name
- System/Application Name
- Whether System/Application contains Confidential or PII data (*Yes/No*)
- EPMO Project ID# (*If applicable*)
- Estimated Corrective Action Cost (*How much it will cost to resolve the deviation*)
- A list of all known Statewide Information Security Standards pertinent to the deviation
- Reason for Deviation (*A detailed description for why the deviation exists*)
- Short Term Risk Mitigation Plan (*Description of steps taken to temporarily mitigate risk*)
- Long Term Risk Mitigation Plan (*Description of steps taken to resolve deviation*)
- Expected Completion Date (*Agency's estimate of when the deviation will be resolved*)

A completed deviation report with all of the above required information must be signed by the agency's IT Manager or CIO and the agency's Security Liaison. Deviation reports may be submitted to the ESRMO via mail, e-mail or fax. **Note:** Deviation reports which lack sufficient information or that are not signed by the authorized agency personnel will be returned to the agency and will need to be resubmitted to the ESRMO.

When an agency submits a deviation report to the ESRMO, the ESRMO will assign a deviation report number to the report, review the report, and provide comments about the deviation. It may be necessary for the ESRMO to request additional information from the agency or to investigate

specific risk mitigation measures related to the reported deviation. Once the ESRMO has the relevant and required information concerning the reported deviation, the ESRMO will provide comments and assign a risk rating (*High, Medium, or Low*) for the deviation. An explanation and examples of the deviation risk ratings are provided below. In addition to the deviation risk rating, the ESRMO will also make a recommendation as to whether the deviation report should be approved or not. This is not the actual approval/denial of the deviation report, but a recommendation to the State CIO. The State Chief Security and Risk Officer (SCSRO) will then sign the deviation report and forward the report with comments to ITS Senior Management for their review and comments.

ITS Senior Management may make additional comments and recommendations for the State CIO to consider. Once ITS Senior Management reviews the deviation report, they will forward the report with their comments to the State CIO. The State CIO may approve the deviation report, deny the deviation report, or return the deviation report to the agency for additional information and/or steps to consider. As part of the review process, the State CIO may require the agency implement specific risk mitigation measures. In addition to the State CIO's comments and approval/denial, a deviation expiration date will also be recorded. This expiration date may not be the same as the estimated expiration date provided by the agency. **Note:** The State CIO's expiration date is the date when the deviation report will expire. The agency shall have the deviation resolved by this date or the agency will be required to submit another deviation report for the State CIO to review.

Deviation Risk Rating

The ESRMO will use the following ratings to rate deviation reports based upon the specific conditions reported in the deviation. The following list includes examples of each risk rating, but is not an all-inclusive list:

High:

- An application or system that stores/processes confidential, personally identifiable information (PII) or regulatory data
- Non-supported application or operating system (OS) software
- Multiple Medium/Low risk deviations

Medium:

- Insufficient patching schedules
- Lack of required security software
- Weak password management
- Weak administrative functions on infrastructure systems
- Insufficient network/application segmentation
- Insufficient separation of duties

Low:

- Extended timeouts

- Insufficient auditing, monitoring or reporting
- Exemptions to telecom law or other statutes or standards not required by the Statewide Information Security Manual
- Other deviations

Deviation Report Monitoring Process

The ESRMO will track all approved deviation reports and will follow up with the agency regarding any specific actions the State CIO may require. The ESRMO will send quarterly summary reports to the agency on all deviation reports the ESRMO is tracking for the agency. The ESRMO will also contact the agency within one month of a deviation report's expiration date to request a status on the agency's deviation. If the agency reports a deviation as being resolved, the ESRMO will record the deviation as closed and will cease monitoring that deviation. If the agency reports a deviation as not being resolved by the deviation report's expiration date, the ESRMO will request the agency to submit a revised deviation report to the ESRMO for review.

Revised deviation reports will follow the same reporting and review process as all other deviation reports. The agency will use the same online deviation reporting form to submit a revised deviation report to the ESRMO for review. When submitting a revised deviation report form, the agency should provide any relevant information on steps already taken to mitigate/resolve the deviation and why the deviation will not be resolved by the deviation report's expiration date. The ESRMO will increment the deviation report number for revised reports to designate the report is a revision of previous reports (i.e. 10.*1*).

As part of the deviation report monitoring process, the ESRMO provides a monthly summary report to the State CIO which lists all Approved, Expired and In Progress deviation reports.

Document History

Initial Release Date:	08/21/2012	Version:	1.0
Date of Last Review:		Version:	1.0
Date Retired:			
Architecture Interdependencies:	N/A		
Reviewer Notes: Version 1.0: created, reviewed and approved by the SCSRO effective 08/21/2012.			

~End of document~